

Corso di Algebra 1 - a.a. 2025-2026

Prova scritta del 16/09/2026

1. Dato un gruppo G e $a \in G$, sia

$$E(a) := \{g \in G : gag^{-1} \in \{a, a^{-1}\}\},$$
$$F(G) := \{a \in G : E(a) = G\}.$$

- (a) Dimostrare che $E(a)$ è un sottogruppo di G .
 - (b) Dimostrare che $Z(G) \subseteq F(G)$.
 - (c) Per $n > 2$ dimostrare che $F(D_n) = \langle R \rangle$.
 - (d) Stabilire se $F(D_3 \times D_3)$ è un sottogruppo di $D_3 \times D_3$.
2. Dato un intero a , sia $f_a := aX^4 + (4 - 2a)X^2 + (a - 4)X + 1$.
- (a) Stabilire se $\mathbb{Z}[X]/(f_0)$ è un dominio.
 - (b) Dimostrare che $\mathbb{Z}[X]/(2, f_a)$ è un campo se e solo se a è dispari.
 - (c) Dimostrare che $\mathbb{Z}[X]/(3, f_1)$ non è un campo e non è isomorfo al prodotto di due campi.
 - (d) Dimostrare che (per ogni a) non esiste un omomorfismo di anelli $\mathbb{Z}[X]/(f_a) \rightarrow \mathbb{Z}$.

Soluzioni

1. (a) $1 \in E(a)$ perché $1a1^{-1} = a$. Dati $g, h \in E(a)$, va poi dimostrato che $gh^{-1} \in E(a)$. Per definizione $gag^{-1} = a^i$ e $hah^{-1} = a^j$ con $i, j \in \{1, -1\}$. Si noti che (essendo il coniugio tramite g un omomorfismo) si ha $ga^k g^{-1} = (gag^{-1})^k = (a^i)^k = a^{ik}$, e analogamente $ha^k h^{-1} = a^{jk}$ per ogni $k \in \mathbb{Z}$. Per $k = j$ quest'ultima uguaglianza diventa $ha^j h^{-1} = a$ (dato che $j^2 = 1$); moltiplicando a sinistra per h^{-1} e a destra per h si ottiene $a^j = h^{-1}ah$. Pertanto

$$gh^{-1}a(gh^{-1})^{-1} = gh^{-1}ahg^{-1} = ga^j g^{-1} = a^{ij}$$

il che dimostra che $gh^{-1} \in E(a)$ (dato che $ij \in \{1, -1\}$).

- (b) Dato $a \in Z(G)$, per definizione si ha $ga = ag$ per ogni $g \in G$. Poiché $ga = ag$ se e solo se $gag^{-1} = a$, si ottiene $gag^{-1} = a$ per ogni $g \in G$. In particolare, questo dimostra che $E(a) = G$, cioè $a \in F(G)$.

- (c) $R^k \in F(D_n)$ (cioè $E(R^k) = D_n$) per ogni $k \in \mathbb{Z}$ perché

$$\begin{aligned} R^i R^k (R^i)^{-1} &= R^i R^k R^{-i} = R^{i+k-i} = R^k, \\ R^i S R^k (R^i S)^{-1} &= R^i S R^k S^{-1} R^{-i} = R^i R^{-k} S S^{-1} R^{-i} = R^{-k} = (R^k)^{-1} \end{aligned}$$

per ogni $i \in \mathbb{Z}$. Dunque $\langle R \rangle \subseteq F(D_n)$, e per concludere basta dimostrare che $R^k S \notin F(D_n)$ (cioè $E(R^k S) \neq D_n$) per ogni $k \in \mathbb{Z}$. In effetti $R \notin E(R^k S)$ perché

$$R R^k S R^{-1} = R R^k R S = R^{k+2} S \notin \{R^k S, (R^k S)^{-1}\} = \{R^k S\}$$

(essendo $n > 2$).

- (d) $F(D_3 \times D_3)$ non è un sottogruppo di $D_3 \times D_3$: si può per esempio verificare che $(R, 1), (1, R) \in F(D_3 \times D_3)$, ma $(R, 1)(1, R) = (R, R) \notin F(D_3 \times D_3)$. Infatti, per quanto visto nel punto precedente, per ogni $g, h \in D_3$ si ha

$$(g, h)(R, 1)(g, h)^{-1} = (gRg^{-1}, h1h^{-1}) = (R^i, 1) = (R, 1)^i$$

con $i = 1$ se $g \in \langle R \rangle$ e $i = -1$ se $g \in D_3 \setminus \langle R \rangle$. Questo dimostra $E((R, 1)) = D_3 \times D_3$, cioè $(R, 1) \in F(D_3 \times D_3)$, e analogamente $(1, R) \in F(D_3 \times D_3)$. D'altra parte $(S, 1) \notin E((R, R))$ (perciò $(R, R) \notin F(D_3 \times D_3)$) perché

$$(S, 1)(R, R)(S, 1)^{-1} = (SRS^{-1}, 1R1^{-1}) = (R^{-1}, R)$$

è diverso sia da (R, R) che da $(R, R)^{-1} = (R^{-1}, R^{-1})$.

2. (a) Poiché $f_0 = 4X^2 - 4X + 1 = (2X - 1)^2$ non è irriducibile nel dominio $\mathbb{Z}[X]$, l'ideale (f_0) non è primo in $\mathbb{Z}[X]$, e dunque $\mathbb{Z}[X]/(f_0)$ non è un dominio.
- (b) Per il terzo teorema di isomorfismo per anelli

$$\mathbb{Z}[X]/(2, f_a) \cong (\mathbb{Z}[X]/(2))/(\overline{f_a}) \cong \mathbb{Z}/2\mathbb{Z}[X]/(\overline{f_a}),$$

con $\overline{f_a} = \overline{a}X^4 + \overline{a}X + \overline{1} \in \mathbb{Z}/2\mathbb{Z}[X]$. Va quindi dimostrato che a è dispari se e solo se $\mathbb{Z}/2\mathbb{Z}[X]/(\overline{f_a})$ è un campo. Tenendo conto che $\mathbb{Z}/2\mathbb{Z}[X]$ è un dominio a ideali principali (essendo $\mathbb{Z}/2\mathbb{Z}$ un campo perché 2 è un numero primo), quest'ultima condizione è soddisfatta se e solo se $\overline{f_a}$ è irriducibile in $\mathbb{Z}/2\mathbb{Z}[X]$. D'altra parte per a pari $\overline{f_a} = \overline{1} \in \mathbb{Z}/2\mathbb{Z}[X]^*$ non è irriducibile, mentre per a dispari $\overline{f_a} = X^4 + X + \overline{1}$ è irriducibile perché è di quarto grado, non ha radici in $\mathbb{Z}/2\mathbb{Z}$ e non è divisibile per $X^2 + X + \overline{1}$ (che è l'unico polinomio irriducibile di secondo grado in $\mathbb{Z}/2\mathbb{Z}[X]$), come è immediato verificare.

- (c) Come nel punto precedente, si ha $\mathbb{Z}[X]/(3, f_1) \cong \mathbb{Z}/3\mathbb{Z}[X]/(\overline{f_1})$, con $\overline{f_1} = X^4 + 2X^2 + \overline{1} = (X^2 + \overline{1})^2 \in \mathbb{Z}/3\mathbb{Z}[X]$. Poiché nell'anello $\mathbb{Z}/3\mathbb{Z}[X]/(\overline{f_1})$ l'elemento $a := X^2 + \overline{1} + (\overline{f_1})$ è tale che $a \neq 0$ e $a^2 = 0$, per concludere basta osservare che in un anello isomorfo a un campo o a un prodotto di due campi non esiste un elemento non nullo il cui quadrato sia nullo.
- (d) Per assurdo esista un omomorfismo (di anelli) $\alpha: \mathbb{Z}[X]/(f_a) \rightarrow \mathbb{Z}$. Indicando con $\pi: \mathbb{Z}[X] \rightarrow \mathbb{Z}[X]/(f_a)$ l'omomorfismo di proiezione al quoziente, si ottiene un omomorfismo $\beta := \alpha \circ \pi: \mathbb{Z}[X] \rightarrow \mathbb{Z}$ tale che $\beta(f_a) = \alpha(\pi(f_a)) = \alpha(\overline{0}) = 0$. Poiché, per ogni anello A , esiste un unico omomorfismo $\mathbb{Z} \rightarrow A$, l'omomorfismo $\beta|_{\mathbb{Z}}: \mathbb{Z} \rightarrow \mathbb{Z}$ deve essere $\text{id}_{\mathbb{Z}}$. Posto $n := \beta(X) \in \mathbb{Z}$, si ha allora

$$\begin{aligned} 0 = \beta(f_a) &= \beta(aX^4 + (4 - 2a)X^2 + (a - 4)X + 1) \\ &= an^4 + (4 - 2a)n^2 + (a - 4)n + 1 = f_a(n), \end{aligned}$$

cioè n è radice di f_a . Per ottenere una contraddizione basta quindi dimostrare che f_a non ha radici intere. In effetti, per il criterio della radice razionale, le eventuali radici intere di f_a possono essere solo 1 o -1. Tuttavia non esiste $a \in \mathbb{Z}$ tale che 1 (rispettivamente -1) sia radice di f_a , cioè (per il teorema di Ruffini) tale che $0 = f_a(1) = 1$ (rispettivamente $0 = f_a(-1) = 9 - 2a$).